UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,585	03/29/2004	Jeffrey A. Aaron	BELL-0340/00379 C1	2073

39072 7590 07/07/2009

AT&T Legal Department - MB
Attn: Patent Docketing
Room 2A-207
One AT&T Way
Bedminster, NJ 07921

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
07/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,585	AARON ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2009 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29,32-35,43-45 and 47-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29,32-35,43-45 and 47-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 13, 2009 has been entered. Claims 29, 32-35, 43-45, 47-52 are pending. Claims 31, 46 are cancelled and Claims 29 and 45 are amended by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 29, 32, 33, 35, 43, 44, 45, 47, 48, 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (US Patent No. 6,415,321) in view of Aucsmith et al (US Pub. No. 2003/0110392) and in view of Sheikh et al (US Pub. No. 2002/0078382).

As per claim 29, Gleichauf teaches:

polling a plurality of devices of the networked computer system for information relating to network communication thereof [col. 6 lines 21-25, col. 5 lines 46-54]; detecting an anomaly at a first device in the computer system from information obtained from at least two devices of the polled plurality of devices of the networked computer system using network-based intrusion detection techniques comprising analyzing data entering

into a plurality of hosts, servers and computer sites in the networked computer system [Fig. 2, col. 5 lines 15-31, 46-67, col. 6 lines 1-4, Fig. 3].

Gleichauf teaches detecting potential vulnerabilities associated with network devices as above. Gleichauf does not expressively mention determining a second device that is anticipated to be affected by the anomaly following the detection of the anomaly and prior to polling of the second device (i.e. possible security problem) [Fig.1, paragraph 0043-0046, 0050, 0051, 0012, 0013].

Aucsmith discloses: detecting an anomaly at a first device in the computer system [Fig. 1, paragraph 0039, 0041, 0043, Fig. 2]; determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device (i.e. possible security problem is detected prior to querying the second device/client) [Fig.1, paragraph 0043-0046, 0050, 0051, 0012, 0013].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Aucsmith with Gleichauf to detect possible anomaly in the network prior to querying the second device (obtaining the information from the second client), since one would have been motivated to protect the resources against unauthorized network access and prevent illicit attempts to access the resources [Aucsmith paragraph 0002].

Gleichauf teaches polling a plurality of devices of the networked computer system as above. Gleichauf doesn't expressively mention polling a plurality of devices of the network computer system in a predetermined scheduled sequential order.

However, in an analogous art, Sheikh teaches: polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof [Fig. 1, 1A, paragraph 0032 lines 5-9, 0033, 0042, Fig. 4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Gleichauf and Sheikh with the teaching of Sheikh, since one would have been motivated to provide cheaper monitoring mechanism, which requires less computing power [Sheikh, paragraph 0042 lines 15-16].

As per claim 32, the rejection of claim 29 is incorporated and Aucsmith teaches:

the anomaly comprises one of an intrusion and an intrusion attempt [paragraph 0027 lines 7-17].

As per claim 33, the rejection of claim 29 is incorporated and Aucsmith teaches:

analyzing a plurality of data packets with respect to predetermined patterns [Fig. 1, paragraph 0039].

As per claim 35, the rejection of claim 29 is incorporated and Aucsmith teaches:

controlling the second device responsive to determining the second device is anticipated to be affected by the anomaly [paragraph 0012, 0013, Fig. 1].

As per claim 43, the rejection of claim 35 is incorporated and Aucsmith teaches: controlling a firewall of the second device responsive to determine the second device is anticipated to be affected by the anomaly [Fig. 1, paragraph 0054, 0057].

As per claim 44, the rejection of claim 35 is incorporated and Aucsmith teaches: Sending an alert to the second device prior to polling of the second device [Fig. 1, paragraph 0012, 0013, 0051].

As per claim 45, it encompasses limitations that are similar to limitations of claim 29. Thus, it is rejected with the same rationale applied against claim 29 above.

As per claim 47, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 32. Thus, it is rejected with the same rationale applied against claim 32 above.

As per claim 48, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 33. Thus, it is rejected with the same rationale applied against claim 33 above.

As per claim 50, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 35. Thus, it is rejected with the same rationale applied against claim 35 above.

As per claim 51, the rejection of claim 50 is incorporated and it encompasses limitations that are similar to limitations of claim 43. Thus, it is rejected with the same rationale applied against claim 43 above.

As per claim 52, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 44. Thus, it is rejected with the same rationale applied against claim 44 above.

3. Claim 34 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (US Patent No. 6,415,321) in view of Aucsmith et al (US Pub. No. 2003/0110392) in view of Sheikh et al (US Pub. No. 2002/0078382) and in view of Wada et al (US Patent No. 7,047,142).

As per claim 34, the rejection of claim 33 is incorporated and Aucsmith teaches analyzing the received the data packet by the device [Fig. 1, paragraph 0025, 0039]. Wada teaches analyzing packets/data by at least two devices in the networked computer system [col. 2 lines 18-23].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wada with Gleichauf, Aucsmith and Sheikh, since one would have been motivated to monitor the various devices for predicting a/an failure/anomaly in the communication network [Wada, col. 1 lines 7-9].

As per claim 49, the rejection of claim 48 is incorporated and it encompasses limitations that are similar to limitations of claim 34. Thus, it is rejected with the same rationale applied against claim 34 above.

Response to Amendment

4. Applicant's arguments filed May 13, 2008 have been fully considered but they are not persuasive.

Regarding to the 35 U.S.C. § 101 rejection, Applicant has amended the specification to delete reference to "a carrier wave embodied in an ....." to correct the 35 U.S.C. 101 issue. Therefore, the 35 U.S.C. 101 rejection is withdrawn.

Regarding to amended claims 29 and 45 limitation "*...detecting an anomaly ...from information obtained from at least two devices of the polled...*", a newly found reference by Gleichauf et al. (US 6,415,321) is used with the previously cited prior art. See new ground of rejection above and therefore, applicant's argument with respect to claims 29 and 45 are moot in view of the new ground of rejection.

Regarding to applicant's argument to claims 29 and 45, the combination of Gleichauf, Aucsmith and Sheikh teaches the claim limitation. Gleichauf teaches the acquisition engine for acquire network information through polling in cooperation with

plurality of network devices. The polling is performed by sending a series of queries to the network devices to determine their response and to collect their own data (e.g. identification of each device types, and its operating system, services and potential vulnerabilities). As shown in Fig. 2, the vulnerabilities rows depict the operating system, services and potential vulnerabilities associated with the device types in the device types rows. Further, Aucsmith discloses a server that propagates any possible security problems seen by any of the client terminals to all of the client terminal so that all of the client terminals can defend against that possible security problem in real time. The server also uses the possible security problems reported by agent to help detect intrusion patterns, new intrusion techniques, and other security problems that may not be apparent to an individual client terminal (i.e. determining a second device that is anticipated to be affected by the anomaly ……..following the detection of the anomaly and prior to detecting at the second device). Further, Skeikh teaches polling the plurality of device of the networked computer system in a predetermined scheduled sequential order for information relating to network communicaitons. Therefore, the combination of Gleichauf, Aucsmith and Sheikh teache the claim subject matter. See detail rejection above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/N. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435